



Lothar Binding  
Mitglied des Deutschen Bundestages

## **Bürgerrechte und Innere Sicherheit**

Vielen Dank für Ihr Schreiben. Sie schildern mir Ihre Angst vor einer Einschränkung ihrer Bürgerrechte. Die staatlichen Ermittlungsbehörden missachten den grundgesetzlichen Schutz der Privatsphäre und überschreiten im Kampf gegen den internationalen Terrorismus und die Organisierte Kriminalität ihre rechtsstaatlich eingehegten Kompetenzen – so lautet oft die Befürchtung. Die verdachtsunabhängige Speicherung von Telekommunikationsdaten, das heimliche Ausspähen der Computerfestplatte oder der polizeiliche Einsatz der Bundeswehr im Inneren sind Szenarien, die bei vielen Bürgerinnen und Bürgern die Angst vor einem Überwachungsstaat nähren, der sie auf Schritt und Tritt misstrauisch beäugt und kontrolliert.

Die Vorstellung, Mails, Telefongespräche oder das Surfen im Internet seien nicht mehr privat, sondern wären den Ermittlungsbehörden zugänglich, ist eine beängstigende Vorstellung – auch für mich. Daher teile ich Ihre grundsätzliche Sorge um die Einschränkung unserer Bürgerrechte bei der Bekämpfung von Terrorismus und Organisierter Kriminalität. Bedenken habe ich besonders bei Themen wie der Onlinedurchsuchung und bei der sog. Vorratsdatenspeicherung.<sup>1</sup>

Präzise Kenntnisse sind für meine eigene Einschätzung dieser juristisch und politisch komplexen Sachlage notwendig. Meine Ausführungen stützen sich daher auf Informationen der zuständigen Arbeitsgruppen der SPD- Fraktion im Deutschen Bundestag sowie auf eigene Recherchen. Auf diesen Grundlagen mache ich mir ein Bild von den Argumenten der Befürworter und Gegner der Vorratsdatenspeicherung und der Onlinedurchsuchung.

Für eine wirksame Verfolgung und Bekämpfung von Straftaten sei der verdeckte Zugriff auf Telekommunikationsdaten und Computerfestplatten Verdächtiger erforderlich, argumentieren die Befürworter der Vorratsdatenspeicherung und der Online- Durchsuchung. Deshalb müsse man diese Daten über einen gewissen Zeitraum einsehen und speichern dürfen. Potentielle Gefahren rechtzeitig erkennen und verdächtige Personen aus dem Verkehr ziehen – so lautet das Ziel für jene Politiker und Behörden, die Verantwortung für unsere Innere Sicherheit übernehmen.

Mit dem Instrument der heimlichen Online- Durchsuchung soll mittels eines eingeschleusten Virusprogramms Daten des PC- Inhabers auf einen Polizeicomputer gespeichert werden, um sie nach belastenden Informationen durchforsten zu können - ohne das Wissen des Betroffenen. Ermittlungsbehörden erhoffen sich von diesem Zugriff auf Computerfestplatten und die sog. Verkehrs- und Standortdaten bei der Telekommunikation

---

<sup>1</sup> Hinweise zu den verwandten Themen RFID (*Radio Frequency Identification*) und der Speicherung biometrischer Daten auf Ausweisdokumenten finden Sie auch an anderer Stelle auf meiner Website.

Erleichterungen bei der Verbrechensbekämpfung. Dabei handelt es sich um Daten, die entstehen, wenn man telefoniert, ein Fax sendet, im Internet surft, sich mit anderen in einem *Chatroom* unterhält oder eine E-Mail verschickt. Sie enthalten Informationen über IP-Adressen, Datum, Uhrzeit und Dauer der Verbindung sowie die dabei übertragene Datenmenge.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betonte hingegen in einer Pressemitteilung vom März 2007, dass die Vorratsdatenspeicherung in Widerspruch zur Verfassung und zur Rechtsprechung des Bundesverfassungsgerichtes stehe. Zudem beeinträchtige sie „die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich“.

Die Frage nach der Erlaubnis zur Vorratsdatenspeicherung und zur Onlinedurchsuchung berührt wichtige Aspekte unseres Staatsverständnisses. Eine der fundamentalen Aufgaben unseres demokratischen Gemeinwesens ist der grundgesetzlich verankerte Schutz der Menschen- und Bürgerrechte. Sie sind ihrem Wesen und Ursprung nach Abwehrrechte gegenüber staatlicher Willkür, bilden die Richtschnur für das gesamte staatliche Handeln und setzen ihm klare Grenzen. In der SPD arbeiten wir für einen solchen demokratischen Rechtsstaat, der die sozialdemokratischen Grundwerte Freiheit, Gerechtigkeit und Solidarität gewährleistet.

Gleichzeitig setzt sich der Rechtsstaat aber auch die Aufgabe, seine Bürgerinnen und Bürger zu schützen, ihr Hab und Gut zu verteidigen und sie vor Angriffen auf ihr leibliches Wohl zu bewahren. Dieses Sicherheitsinteresse ist eine der zentralen Herausforderungen des modernen Staates. Zu diesem Zweck verfügt er bereits über wirksame Instrumente der Strafverfolgung und der Gefahrenabwehr, die die Grenzen, die das Grundgesetz setzt, respektieren.

Beide Aufgaben – Schutz der bürgerlichen Freiheiten und Verantwortung für die innere und äußere Sicherheit - haben ihre normative Berechtigung. Zum Dilemma werden sie allerdings in einer Entscheidungssituation, in der die Verfolgung eines Ziels nur auf Kosten des anderen gelingen kann.

Die Gruppe für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, die sog. Artikel 29- Datenschutzgruppe der Europäischen Union, hat eine treffende Formulierung für dieses Dilemma gefunden:

„Die Aufbewahrung von Verkehrsdaten ist ein Eingriff in das unverletzliche Grundrecht auf Achtung des Brief-, Post- und Fernmeldegeheimnisses. Eingriffe in dieses Grundrecht müssen einem zwingenden Bedarf entspringen, sie sollten nur in Ausnahmefällen gestattet werden und angemessenen Schutzmaßnahmen unterworfen sein. Der Terrorismus stellt unsere Gesellschaft vor eine reale und drängende Herausforderung. Die Regierungen müssen auf diese Herausforderung in einer Form reagieren, die dem Bedürfnis der Bürger, in Frieden und Sicherheit zu leben, wirkungsvoll nachkommt, ohne die Menschenrechte des Einzelnen, darunter das Recht auf Privatsphäre und Datenschutz, auszuhöhlen, denn diese Rechte gehören zu den Eckpfeilern unserer demokratischen Gesellschaft.“<sup>2</sup>

Ein Staat, der nicht in der Lage ist, seine Bürger vor terroristischen Angriffen und kriminellen Machenschaften zu schützen, hat schwerwiegende Defizite aufzuweisen. Wo der Schutz der

---

<sup>2</sup> Artikel 29- Datenschutzgruppe, 1868/05/DE. In ähnlicher Weise argumentiert auch der Europäische Datenschutzbeauftragte.

Bürger jedoch nur durch die Außerkraftsetzung der Menschen- und Bürgerrechte gelingt, stehen wir vor ernsthaften Legitimationsproblemen.

Die Balance zwischen diesen beiden Zielvorgaben zu finden, ist schwierig. Nicht immer komme ich bei politischen Entscheidungen zu einer Position, die für beide Seiten eine *win-win*- Situation darstellt und meine volle Zustimmung hat. Gelegentlich muss ich zwischen Zielen abwägen, die in einem Spannungsverhältnis zueinander stehen – und bisweilen lassen sich für juristisch komplexe und politisch sensible Probleme keine einfachen Lösungen finden, die alle Seiten zufriedenstellen.

Der rasante Übergang ins Informationszeitalter bietet Ermittlungsbehörden neue Möglichkeiten, Gesetzesverstöße aufzuspüren, zu verfolgen und zu ahnden. Allerdings muss man dabei auf Ausgewogenheit und Verhältnismäßigkeit der Mittel achten. Denn nicht alles, was technisch machbar ist, ist meines Erachtens auch politisch sinnvoll und rechtlich zulässig. Wo Daten, die den Kernbereich der privaten Lebensgestaltung betreffen, gespeichert werden bzw. dem Zugriff der Ermittler offenstehen sollen, stößt das Strafverfolgungsinteresse des Staates in einen sensiblen Bereich vor. Diese Daten müssen durch ein absolutes Verwertungsverbot geschützt werden. Denn die Grundrechte und politischen Prinzipien des Rechtsstaates sind keine Variablen, die je nach Sicherheitslage und Bedrohungsszenario neu festgelegt werden können.

Diese unbedingte Schranke für Ermittlungsbehörden hat das Bundesverfassungsgericht definiert und gestärkt. Im Jahr 2005 etwa hat das Bundesverfassungsgericht das Umsetzungsgesetz zum EU- Haftbefehl und die Telefonüberwachung nach niedersächsischem Landesrecht für unvereinbar mit dem Grundgesetz erklärt. Auch die SPD- Bundestagsfraktion verteidigt diese Linie und hat die geplante Vorratsdatenspeicherung von Fingerabdrücken, die zur Erstellung biometrischer Pässe genommen wurden, abgelehnt.

Bei der gegenwärtig debattierten Online- Durchsuchung lässt sich das Spannungsverhältnis zwischen Sicherheitsbedürfnis und Grundrechtsschutz exemplarisch nachzeichnen. Das Fernmelde- und Postgeheimnis wird in Artikel 10 des Grundgesetzes geschützt. Der Bundesgerichtshof ist der Maxime des Bundesverfassungsgerichtes gefolgt und hat die Praxis der Online- Durchsuchung verboten, da keine ausreichende gesetzliche Grundlage vorhanden war. Gegenwärtig befassen sich die Rechtspolitiker im zuständigen Ausschuss damit, dieses Ermittlungsinstrument auf eine grundgesetzkonforme Basis zu stellen. Die SPD- Bundestagsfraktion setzt sich für die enge Umschreibung des Anwendungsbereiches ein: Online- Durchsuchungen sollen höchstens zur Abwehr einer konkreten Gefahr, nicht aber zur Prävention zulässig sein.

Denn das staatliche „Ausspähen“ von Festplatten ist ein virtuelles Eindringen in Wohnung und Privatsphäre. Schließlich darf man nicht vergessen, dass viele Computernutzer auch persönliche Informationen auf ihren Festplatten abspeichern, bspw. Kontodaten, Bilder, Krankenunterlagen, Tagebücher etc. Das Bundesverfassungsgericht nennt in seiner Rechtsprechung diesen Bereich „das letzte Refugium zur Wahrung der Menschenwürde“.

Ihn zu verteidigen und auszudehnen, haben wir uns auch bei der Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung vorgenommen. Die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates ist am 3. Mai 2006 in Kraft getreten. Sie muss für Verkehrsdaten der Festnetz- und Mobilfunktelefonie bis zum 15. September 2007 in nationales Recht umgesetzt sein; für Internetverkehrsdaten ist ein Aufschub bis 15. März 2009

zulässig. Bundesregierung und Bundestag arbeiten gegenwärtig bei der Ausarbeitung dieses sog. Umsetzungsgesetzes eng zusammen.

Konkret ist geplant, die Umsetzung der Richtlinie mit datenschutzrechtlichen Urteilen des Bundesverfassungsgerichtes und Klarstellungen in der Strafprozessordnung zu verbinden. Die Regierung hat einen Gesetzentwurf zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen vorgelegt. Der Entwurf wurde am 6. Juli 2007 in erster Lesung im Bundestag eingebracht und anschließend an die beteiligten Ausschüsse zur weiteren Beratung überwiesen. Es handelt sich um den federführenden Rechtsausschuss sowie die mitberatenden Ausschüsse für Inneres und Ernährung, Landwirtschaft und Verbraucherschutz. Wir haben uns gemeinsam mit unserem Koalitionspartner dafür eingesetzt, dass bei der Umsetzung der Richtlinie in nationales Recht keine Regelungen zu Speicherdauer und erfassten Datenarten getroffen werden, die über die Mindestanforderungen der Richtlinie hinausgehen. Diese Selbstbindung hatten wir auch im Koalitionsvertrag festgeschrieben.

Die wesentlichen Eckpunkte des EU- Kompromisses, für die wir einen vernünftigen Ausgleich zwischen Grundrechtsschutz und Strafverfolgung finden wollen, sind folgende:

- Es ist eine **Mindestspeicherfrist** von 6 Monaten vorgesehen, eine Verlängerung der Frist auf bis zu 24 Monate liegt im Ermessen der einzelnen Mitgliedstaaten. Der Bundestag hat bekräftigt, dass nicht über die Mindestspeicherdauer von sechs Monaten hinausgegangen werden soll. Der von der Richtlinie vorgegebene Spielraum von bis zu 24 Monaten wird also nicht ausgeschöpft werden. Auch heute schon können Unternehmen nach dem Telekommunikationsgesetz Daten bis zu sechs Monate lange aufbewahren, um sie zur Rechnungslegung verwenden zu können. Was sich allerdings ändert, ist folgendes: aus der Erlaubnis für Unternehmen zur Speicherung von Daten wird durch die europäische Richtlinie eine Verpflichtung. In der Praxis bedeutet dies, dass die Unternehmen, die schon heute in der Regel drei Monate speichern, diesen Zeitraum um lediglich drei Monate verlängern müssen.
- **Speicherzweck und Datenabfrage** sind auf Zwecke der Strafverfolgung, d.h. die Ermittlung, Aufdeckung und Verfolgung von Straftaten von erheblicher Bedeutung sowie von mittels Telekommunikation begangener Straftaten beschränkt. Für diese Daten muss ein tatsächlicher Bedarf vorliegen, und die Speicherung darf keinen unverhältnismäßigen Aufwand verursachen. Für letztgenannte Fallgruppe ist dies jedoch nur dann zulässig, wenn die Erforschung des Sachverhalts auf andere Weise ausgeschlossen ist; zudem muss die Datenerhebung in angemessenem Verhältnis zur Bedeutung der Sache stehen. Das deutsche Recht sieht schon heute vor, dass Behörden bei Vorliegen der genannten gesetzlichen Voraussetzungen, wie bei der Verbreitung von kinderpornographischer oder fremdenfeindlicher Inhalte im Internet, Auskünfte von Telekommunikationsunternehmen einfordern können. Dazu benötigen sie einen richterlichen Beschluss und müssen bestimmte Verfahrensvorschriften einhalten. Daran wollen wir festhalten. Meiner Ansicht nach muss sichergestellt sein, dass mit der Vorratsdatenspeicherung nur solche schwerwiegenden Taten verfolgt werden, für deren Aufklärung die Telekommunikationsüberwachung besonders unerlässlich ist. Sie darf nicht zu einem „normalen“ Instrument der Strafverfolgung werden.
- **Standort- und Verbindungsdaten**, wie Telefonnummern von Handys und Festnetzgeräten, werden nur für den Beginn des Mobilfunkverkehrs, nicht auch für das Ende gespeichert, um die Speicherkosten zu senken. Erfolgreiche Anrufversuche werden

nicht aufgezeichnet. Es werden lediglich Internet-Einwahldaten, d.h. die IP- Adresse und der Einwahlzeitpunkt, sowie Verkehrsdaten zu Emails und Internettelefonie aufgezeichnet. Inhalte der vom Nutzer aufgerufenen Seiten und der Kommunikation werden ausdrücklich nicht protokolliert. Die Neuregelung sieht vor, diese Daten vielen Behörden zum Online-Abruf zur Verfügung zu stellen. Dazu gehören Polizei, Staatsanwaltschaft, Nachrichtendienste, Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht, kurz BaFin. Allerdings hege ich an dieser Stelle auch deutliche datenschutzrechtliche Bedenken, wenn Nutzer öffentlich zugänglicher E-Mail-Dienste zur Angabe ihres Namens und ihrer Adresse verpflichtet werden.

Bezüglich der Ausweitung der Kompetenzen und Aufgabengebiete der Bundeswehr im Inneren gilt für mich die Aussage des Koalitionsvertrages, der auf S. 135 „die grundsätzliche Trennung zwischen polizeilichen und militärischen Aufgaben“ festhält. Überlegungen, der Bundeswehr weitreichende Befugnisse im präventiven Bereich, bspw. beim Objektschutz, und im reaktiven Bereich bei der Katastrophenabwehr zu geben, lehne ich ab. Denn es ist ein fundamentaler Unterschied, ob die Bundeswehr zur Abwehr eines schweren Unglücksfalles oder einer Katastrophe sowie bei der Bewältigung der Folgen eingesetzt wird – dies ist nach geltendem Recht und im Einklang mit unserer Verfassung möglich -, oder ob sie ohne konkrete Gefährdung „zur Verhinderung einer Katastrophe oder eines Terroranschlags“ eingesetzt wird – das ist eine der zentralen Forderungen der Union.

Der grundsätzliche Einsatz der Bundeswehr im Innern widerspricht den bestehenden verfassungsrechtlichen Festlegungen der Bundesrepublik Deutschland. Unser Grundgesetz ist vom Gedanken des Schutzes der Menschen- und Bürgerrechte durchdrungen und bietet einen sorgsam austarierten Kompromiss zwischen Grundrechtsschutz und den Erfordernissen einer wehrhaften Demokratie. Diesen sollte man nicht ohne Not aus dem Gleichgewicht bringen.

Sicherlich stimmt der Hinweis auf eine veränderte Gefahrenlage im Zeichen eines weltweit operierenden Terrorismus, zerfallender Staaten und einer Aufweichung der Trennung zwischen Innerer und Äußerer Sicherheit. Allerdings bin ich skeptisch, ob eine Grundgesetzänderung und die Übertragung polizeilicher Aufgaben auf die Bundeswehr darauf die richtige Antwort sind. Ich bezweifle, ob die Bundeswehr über geeignete Fähigkeiten zur Terrorismusbekämpfung verfügt.

Polizei und Nachrichtendienste sind dafür ausreichend legitimiert und ausgestattet. Sie müssen mit Aufklärung und Vorsorgemaßnahmen verhindern, dass es zu Terroranschlägen kommt. Dazu verfügen die Behörden über die Möglichkeit, ein Einreiseverbot für sog. Gefährder auszusprechen; die Anti- Terror- Datei sammelt Informationen über Terrororganisationen und ihre mutmaßlichen Unterstützer; die Speicherung biometrischer Daten in Ausweisen und Pässen verbessert die Möglichkeiten, Verdächtige leichter zu identifizieren. Für die Ahndung von Gesetzesverstößen ist unsere Justiz zuständig. Die Bundeswehr zu einem Instrument des Bundes auszubauen, das auch im Inneren mit deutlich erweiterten Befugnissen eingesetzt werden kann, stellt meines Erachtens keine befriedigende und Problem angemessene Lösung dar. Dieser Schritt würde unsere Sicherheitsarchitektur zerstören und zahlreiche rechtliche, politische und finanzielle Probleme nach sich ziehen. Eine solche Änderung würde sich schnell als Einfallstor für immer neue Ausweitungen des Einsatzes des Militärs im Inneren und einer zunehmenden Militarisierung der Innenpolitik erweisen.

Auch mit der Sicherheit der elektronischen Stimmabgabe haben wir uns im Bundestag schon eingehend beschäftigt. Der Petitionsausschuss des Deutschen Bundestages hat sich in einer

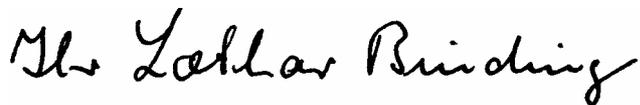
öffentlichen Sitzung am 18. Juni 2007 dieses Themas angenommen; eine endgültige Entscheidung liegt allerdings noch nicht vor. Wie viele meiner Kolleginnen und Kollegen bin ich von der Manipulationssicherheit elektronischer Wahlmaschinen nicht überzeugt.

Die unbedingte Gültigkeit des Wählerwillens ist ein zentrales Funktionsprinzip einer Demokratie. Das an sich verständliche Interesse der Verwaltungsbehörden an einer Vereinfachung und Beschleunigung der Auszählung ist meines Erachtens nachrangig gegenüber der Gefahr einer Verfälschung des Wählerwillens. Wir verfügen in der Bundesrepublik mit dem System der Wahlurnen über einen bewährten Wahlmechanismus, der nicht ohne triftigen Grund abgeschafft werden sollte. Die Kontrolle der Stimmzettel durch Wahlvorstände genießt für mich aus demokratietheoretischen und rechtlichen Gründen Vorrang gegenüber dem Vertrauen in die Hersteller der Wahlmaschinen und das fehlerfreie Arbeiten ihrer technischen Produkte.

Effektive Strafverfolgung und Grundrechtsschutz zugleich zu gewährleisten, ist eine Aufgabe, die große Wachsamkeit und Besonnenheit erfordert. Ich vertraue fest darauf, dass meine Kolleginnen und Kollegen, die in den federführenden Ausschüssen diese Angelegenheiten beraten, sich dieser Verantwortung bewusst sind und eine Regelung finden werden, die einen sinnvollen und praktikablen Ausgleich zwischen diesen beiden Zielen schafft.

In der Hoffnung, dass ich Ihre Bedenken konstruktiv reflektieren und Ihnen einen Einblick in meine Überlegungen geben konnte, verbleibe ich

mit freundlichen Grüßen

A handwritten signature in black ink, reading "Mr. Lothar Binding". The script is cursive and fluid, with the first letters of "Mr.", "Lothar", and "Binding" being capitalized and prominent.

Lothar Binding